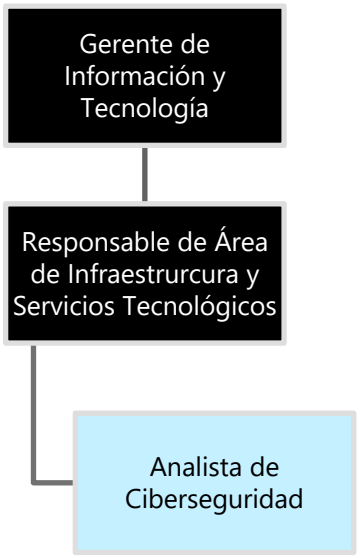
DESCRIPTOR Y PERFIL DEL PUESTO

1. Identificación del Cargo

Nombre del cargo	Analista de Ciberseguridad
Área Organizativa	Gerencia de Información y Tecnología
Reporta a	Responsable de Área de Infraestructura y Servicios Tecnológicos
Supervisa a	No aplica
Cargos que pueden reemplazar su ausencia	No identificados
Familia	Analistas Técnicos
Modalidad de trabajo	Presencial y teletrabajo



Relaciones de Clientes Relevantes	
Cliente interno	**Objetivo principal del servicio**
Todas las áreas del EOR	Brindar servicios tecnológicos relacionados a ciberseguridad y garantizar la óptima operatividad de los esquemas de ciberseguridad implementados.
Cliente externo	**Objetivo principal del servicio**
Agentes del MER OS/OM de América Central, CRIE, proveedores y otras entidades externas.	Brindar servicios tecnológicos especializados relacionados a ciberseguridad.

2. Propósito clave

Administrar y asegurar la operatividad de la infraestructura de ciberseguridad del EOR, con base a las mejores prácticas de la seguridad de la información y de acuerdo con las necesidades de la institución.

3. Funciones principales

Función	Descripción o Responsabilidades
1. Administrar el funcionamiento de la Infraestructura de Ciberseguridad (Firewalls), de acuerdo con los requerimientos internos y externos, nacionales e internacionales.	1.1. Administración de equipos Firewalls de la institución. 1.2. Realizar actividades de gestión de riesgos de la información (planificación, detección y mitigaciones). 1.3. Ejecutar todas las políticas de ciberseguridad a nivel de redes mediante la configuración y administración del Firewall. 1.4. Administrar privilegios y perfiles de acceso a los diferentes sistemas (video vigilancia, telecomunicaciones, control de asistencia del personal, telefonía, climatización y otros). 1.5. Realizar análisis de riesgos previo a la implementación de nuevas tecnologías y con base a dicho análisis, aplicar las reglas de ciberseguridad necesarias. 1.6. Desarrollo de Políticas y protocolos de ciberseguridad institucional. 1.7. Realizar test de intrusión. 1.8. Establecer y verificar los esquemas de ciberseguridad de los servicios web, de acuerdo con normas internacionales. 1.9. Resolver las problemáticas inherentes al funcionamiento de los equipos de ciberseguridad firewalls.
2. Administración y monitoreo de los equipos de ciberseguridad instalados por el EOR en la red regional de comunicación para identificar vulnerabilidades de acceso y desarrollar medidas de ciberseguridad.	2.1. Administración de equipos de ciberseguridad en la redes regionales de comunicación. 2.2. Administrar la infraestructura de ciberseguridad implementado para la comunicación ICCP con los OSOM. 2.3. Administración y mejoras de los mecanismos de ciberseguridad empleados en la comunicación de voz regionales. 2.4. Monitoreo de vulnerabilidades en los enlaces de comunicación de datos y voz regionales. 2.5. Realizar mantenimiento preventivo y correctivo de los equipos de ciberseguridad implementados para la comunicación de datos y voz Regionales. 2.6. Mitigación de las vulnerabilidades identificadas. 2.7. Tomar acciones correctivas ante la falla de los equipos de ciberseguridad.
3. Administración y monitoreo de la herramienta SIEM de Ciberseguridad, así como desarrollo de medidas para la mitigación de riesgos de ciberseguridad.	3.1. Formulación e implementación de políticas y protocolos de ciberseguridad para los Servicios Web. 3.2. Administración y gestión de la infraestructura SIEM para garantizar su disponibilidad continua. 3.3. Análisis de los datos recopilados para detectar actividades sospechosas o anomalías de ciberseguridad a través de la herramienta SIEM.

Función	Descripción o Responsabilidades
	3.4. Generación de informes detallados para proporcionar una visibilidad clara del estado de ciberseguridad. 3.5. Aplicación de técnicas de correlación de eventos para identificar patrones y relaciones entre los incidentes registrados por el SIEM. 3.6. Revisión periódica de las configuraciones y reglas de ciberseguridad para garantizar su eficacia.
4. Administración de herramientas especializadas de ciberseguridad.	4.1. Administración de herramienta de doble factor de autenticación. 4.2. Administración de perfiles de acceso a través de VPN. 4.3. Administración de herramienta de seguridad de equipos corporativos (antivirus). 4.4. Administración de sistema análisis de eventos de ciberseguridad a través de plataforma especializada. 4.5. Administración del portal de inteligencia de amenazas. 4.6. Ejecución de campañas de Phishing. 4.7. Realización de campañas de concientización entre el personal. 4.8. Participar en la evaluación de factibilidad técnica para la adquisición de tecnología y servicios en ciberseguridad, de acuerdo con requerimientos de la institución para atender sus procesos técnicos, comerciales y corporativos.
5. Otras funciones del cargo	5.1. Participar en la disponibilidad informática 7x24 para atender emergencias. 5.2. Preparar informes de gestión e informes técnicos, de acuerdo con requerimientos del jefe inmediato. 5.3. Participar en la evaluación de factibilidad para la adquisición de tecnología y servicios Informáticos, de acuerdo con requerimientos de las diferentes áreas del EOR y del MER u otra área funcional del EOR. 5.4. Realizar cualquier otra tarea encomendada por el jefe inmediato o Gerente de Información y Tecnología, que sea de apoyo para otra área de la misma gerencia u otra área funcional del EOR. 5.5. Proveer Soporte técnico a los colaboradores del EOR en actividades variadas.

4. Competencias conductuales

Tipo	Competencia

Genéricas	Trabajo en equipo
	Gestión de la creatividad e innovación
	Eficacia y orientación a resultados
	Gestión del Cambio
	Enfoque de Atención al Cliente
Personales	Disponibilidad, tenacidad y proactividad
	Habilidad y actitud de aprendizaje
	Orientación por el orden, la calidad y la precisión
	Disciplina y apego a normas y procedimientos
	Manejo del estrés y la presión
	Comunicación efectiva
	Manejo de Relaciones Humanas
Técnicas	Credibilidad técnica

5. Requisitos técnicos

Educación	Indispensable	Deseable
Formación académica	Ingeniero en Telecomunicaciones, en Administración de Redes ó Computación, Ingeniero en Sistemas o Ingeniero ó Licenciado en Ciencias de la Computación o carreras afines.	Maestría en Ciberseguridad
Posgrados, diplomados y/o cursos	– Certificación en soluciones de Fortinet FCSS Certificación de Fortinet FCP	Certificación CCNAv7 Cisco

Experiencia	Tipo cargo	Años	Tipo de organización o rubro
Indispensable	Especialista en Ciberseguridad. Ingeniero en Ciberseguridad. Analista de Ciberseguridad Senior. Ingeniero de Seguridad de Redes. SOC	2-3 en total	Organizaciones grandes / regionales. Organizaciones especializadas en ciberseguridad Organizaciones del sector eléctrico (Administradores de sistema y empresas trasmisoras de energía)

Otros Requisitos	
Manejo empírico del área funcional	– Administración de equipos Firewalls – Administración y configuración de swtiches capa 3 – Experiencia en implementación de esquemas de ciberseguridad, segmentación de redes y ruteos dinámicos. – Experiencia específica mínima de 2-3 años en total, en: Administración de servidores, redes LAN/WAN y Sistemas Operativos de Redes LINUX/UNIX/Windows de Servidor.
Manejo de tecnología e información	– Manejo de tecnologías en la nube AWS, Azure, otras. – Manejo de herramientas de virtualización HyperV, VirtualBox, VmWare. – Manejo de equipos de ciberseguridad FORTINET (Firewalls, Switches, Analizer, AP´s, entre otras)
Conocimientos y habilidades específicas	– Conocimientos de tecnología CISCO WEBEX para reuniones remotas. – Conocimiento de Plataforma Microsoft 365 Business.

	– Conocimientos de tecnología FORTINET. – Conocimientos de tecnología CISCO Switch Core. – Tecnología de Telecomunicaciones.
Manejo de un segundo idioma	– Deseable nivel avanzado de inglés (lectura y escritura).

Fecha de revisión y actualización: Noviembre, 2024.